Hewlett Packard Enterprise

ArcSight Enterprise Security Solutions Architecture H7G99S

HP ArcSight Enterprise Security Solutions Architecture covers design and implementation considerations of a complete enterprise SIEM deployment. This course provides participants with hands-on activities based on a practical solutions-based approach to address common business requirements. Methodologies, terms and concepts are explored in progressive examples using built-in product configuration and management facilities. Product architectures are coupled with deployment best-practices in the context of the HP ArcSight product line as a complete log management and event correlation platform.

ArcSight Enterprise Security Solutions Architecture	
Price	USD $4,000
Links to local schedules, pricing and registration	**US/Canada** **Mexico/Latin America** **Brazil**
HP course #	H7G99S
Category	Security
Duration	5 days

Audience

This advanced course is intended for IT security experts seeking multi-product configuration/ integration and practical deployment methodologies for ArcSight Solutions.

Prerequisites

The attendees of this course must have successfully accomplished:

- HP ArcSight ESM Security Analyst (AESA - formerly ACSA) course or have equivalent hands-on experience
- HP ArcSight ESM Administration (AEIA formerly ACIA) course or have equivalent hands-on experience
- Logger Administration and Operations course or have equivalent hands-on experience

To maximize your learning in this course, we strongly recommend you have accomplished:

- Use Case Foundations Course or have equivalent hands-on experience
- Building Advanced Content course or have equivalent hands-on experience
- Flex Connector Configuration course or have equivalent hands-on experience

During the training, you will learn to:

- Determine appropriate Logger/ESM architecture to address specific log management requirements
- Integrate Logger/ESM in peering and hierarchical deployments
- Optimize ArcSight SmartConnector configurations for a Logger/ESM integrated environment

Course objectives

At the end of this course, you will be able to:

- Identify types of criteria used to define system requirements
- Present a thorough compilation of the various architectures and the pros and cons of each
- Identify integration capabilities and best practices for each product
- Identify data sources and ESM resources required to fulfill the objectives of the use case
- Present multiple real-world scenarios that will be the basis of a complete implementation exercise

Course outline

Module 1: Basic ESM Architecture

- Architecture Overview
- SmartConnector Configuration Utilities
- ESM SSL Communications
- ESM Connector Management
- Best Practices for Common SmartConnectors

Module 2: Multi-Destination Architecture

- Architecture Overview
- Logger/ESM Configuration
- SmartConnector Configuration
- Network Model Implications

Module 3: ESM to Logger Architecture

- Architecture Overview
- ESM Forwarding Connector
- ESM Integration Commands

Module 4: Logger to ESM Architecture

- Architecture Overview
- Logger Forwarding to ESM
- Correlation Event Loopback
- ESM AUP Master
- Network Model Implications

Module 5: Parallel Logger and ESM Architecture

- Architecture Overview
- Logger Peering

Module 6: Tiered ESM Architecture

- Architecture Overview
- ESM Forwarding to ESM
- Logger Audit Forwarding
- Network Model Implications

Module 7: Global Master ESM Architecture

- Architecture Overview
- Parallel ESM Global Master Forwarding
- Global Correlation Rules and Filtering
- Global Correlation Loopback to Logger
- Network Model Implications

Learn more at

hpe.com/us/training/security

H7G99S Ver A.00

c04723046 June 2015

Hewlett Packard Enterprise